UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA - v. – AHMED MOHAMMED EL GAMMAL, a/k/a "Jammie Gammal," Defendant.	15 Cr. 588 (ER)

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANT'S PRETRIAL MOTION TO SUPPRESS, AND FOR THE DISCLOSURE OF FISA ORDER, APPLICATION, AND RELATED MATERIALS

TABLE OF CONTENTS

I. Introduction 1
A. Background 2
B. Overview of the FISA Authorities 3
1. **[CLASSIFIED MATERIAL REDACTED]** 3
2. The FISC's Findings 3
II. The FISA Process 3
A. Overview of FISA 3
B. The FISA Application 6
1. The Certification 8
2. Minimization Procedures 9
3. Attorney General's Approval 9
C. The FISC's Orders 10
III. District Court Review of FISC Orders 14
A. The Review Is to Be Conducted *in Camera* and *ex Parte* 15
1. *In Camera, Ex Parte* Review is the Rule 16
2. *In Camera, Ex Parte* Review is Constitutional 20
B. The District Court's Substantive Review 22
1. Standard of Review 22
2. Probable Cause Standard 23
3. Standard of Review of Certifications 23
4. FISA is Subject to the "Good-Faith" Exception 25
IV. The FISA Information Was Lawfully Acquired and the Physical Search(es) Was/Were Made in Conformity with an Order of Authorization or Approval 27
A. The Instant FISA Application(s) Met FISA's Probable Cause Standard 27
1. **[CLASSIFIED MATERIAL REDACTED]** 27
2. **[CLASSIFIED MATERIAL REDACTED]** 27
a. **[CLASSIFIED MATERIAL REDACTED]** 27
b. **[CLASSIFIED MATERIAL REDACTED]** 27
c. **[CLASSIFIED MATERIAL REDACTED]** 27
d. **[CLASSIFIED MATERIAL REDACTED]** 27
e. **[CLASSIFIED MATERIAL REDACTED]** 27
3. **[CLASSIFIED MATERIAL REDACTED]** 27
B. The Certifications Complied with FISA 28
1. Foreign Intelligence Information 28
2. "A Significant Purpose" 28
3. Information Not Reasonably Obtainable Through Normal Investigative Techniques 28
C. The Physical Search(es) Was/Were Conducted in Conformity with an Order of Authorization or Approval 28
1. The Standard Minimization Procedures 28
2. The FISA Information Was Appropriately Minimized 33
V. The Court Should Reject the Defendant's Legal Arguments 33
A. The FISA Information Should Not Be Suppressed 34
1. **[CLASSIFIED MATERIAL REDACTED]** 34

2. The FISA Application(s) Were Not Based Solely on Protected First Amendment Activity 34
3. A Significant Purpose of the FISA Physical Search(es) Was the Collection of Foreign Intelligence Information and the Certification(s) Complied with FISA 35
4. The Defendant Has not Established Any Basis for the Court to Conduct a *Franks* Hearing 35
5. The Government Complied with the Standard Minimization Procedures 36
B. There Should be No Disclosure of FISA Materials to the Defendant or His Counsel 36
1. Due Process Does Not Require Disclosure 37
2. A Security Clearance Does Not Entitle Defense Counsel to the FISA Materials 41
VI. Conclusion: There Is No Basis to Disclose FISA Materials or to Suppress the FISA Information 44

TABLE OF AUTHORITIES

FEDERAL CASES

ACLU Found. of So. Cal. v. Barr,
952 F.2d 457 (D.C. Cir. 1991).....20, 21, 41

Al-Kidd v. Gonzalez,
2008 WL 5123009 (D. Idaho).....42-43

Brady v. Maryland,
373 U.S. 83 (1963).....41

CIA v. Sims,
471 U.S. 159 (1985).....19

Franks v. Delaware,
438 U.S. 154 (1978).....23, 36, 37

Halperin v. CIA,
629 F.2d 144 (D.C. Cir. 1980).....19-20

In re Grand Jury Proceedings of the Spec. Apr. 2002 Grand Jury,
347 F.3d 197 (7th Cir. 2003).....17-18, 24

In re Kevork,
634 F. Supp. 1002 (C.D. Cal. 1985), *aff'd*,
788 F.2d 566 (9th Cir. 1986).....18, 30

In re Sealed Case,
310 F.3d 717 (Foreign Int. Surv. Ct. of Rev. 2002).....29, 30

In re Terrorist Bombing in East Africa,
552 F.3d 157 (2d Cir. 2008).....42

Ivanov v. United States,
419 U.S. 881 (1974).....45

Massachusetts v. Sheppard,
468 U.S. 981 (1984).....26

Phillippi v. CIA,
655 F.2d 1325 (D.C. Cir. 1981).....19

Rivera v. United States,
928 F.2d 592 (2d Cir. 1991).....37

Scott v. United States,
436 U.S. 128 (1978) 31-32

United States v. Abu-Jihaad,
531 F. Supp. 2d 299 (D. Conn. 2008), *aff'd*,
630 F.3d 102 (2d Cir. 2010) ..... *passim*

United States v. Ahmed,
No. 1:06-CR-147, 2009 U.S. Dist. Lexis 120007
(N.D. Ga. Mar. 19, 2009) 22, 26, 46

United States v. Amawi,
2009 WL 961143 (N.D. Ohio) 43

United States v. Badia,
827 F.2d 1458 (11th Cir. 1987) 23, 24, 25

United States v. Belfield,
692 F.2d 141 (D.C. Cir. 1982) 16, 17, 20, 37, 41

United States v. Benkahla,
437 F. Supp. 2d 541 (E.D. Va. 2006) 21

United States v. Bin Laden,
126 F. Supp. 2d 264 (S.D.N.Y. 2000) 29, 30, 42

United States v. Butenko,
494 F.2d 593 (3d Cir. 1974) 45

United States v. Campa,
529 F.3d 980 (11th Cir. 2008) 23, 24, 25

United States v. Cavanagh,
807 F.2d 787 (9th Cir. 1987) 23

United States v. Colkley,
899 F.2d 297 (4th Cir. 1990) 36, 37

United States v. Damrah,
412 F.3d 618 (6th Cir. 2005) 21, 45

United States v. Daoud,
12 CR-723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014)
755 F.3d 479 (7th Cir. 2014) 17, 39, 43

United States v. Duggan,
743 F.2d 59 (2d Cir. 1984) 16, 17, 23, 24, 25, 36, 39, 40

United States v. Duka,
671 F.3d 329 (3d Cir. 2011) 15, 23, 25

United States v. El-Mezain,
664 F.3d 467 (5th Cir. 2011) 15, 16, 17, 21, 23, 43

United States v. Falcone,
364 F. Supp. 877, 886 (D. N.J. 1973), *aff'd*,
500 F.2d 1401 (3rd Cir. 1974) 32, 33

United States v. Falvey,
540 F. Supp. 1306 (E.D.N.Y. 1982) 39

United States v. Garcia,
413 F.3d 201 (2d Cir. 2005) 25

United States v. Gowadia,
No. 05-00486, 2009 WL 1649714
(D. Haw. June 8, 2009) 21, 41

United States v. Hammoud,
381 F.3d 316 (4th Cir. 2004), *rev'd on other grounds*,
543 U.S. 1097 (2005), *op. reinstated in pertinent part*,
405 F.3d 1034 (4th Cir. 2005) 30, 31, 32

United States v. Isa,
923 F.2d 1300 (8th Cir. 1991) 16, 17, 20, 32

United States v. Islamic Am. Relief Agency,
No. 07-00087-CR-W-NKL, 2009 WL 5169536
(W.D. Mo. Dec. 21, 2009) 19, 24, 25, 32

United States v. Jayyousi,
No. 04-60001, 2007 WL 851278 (S.D. Fla. Mar. 15, 2007), *aff'd*,
657 F.3d 1085 (11th Cir. 2011) 21

United States v. Kashmiri,
No. 09-CR-830-4, 2010 WL 4705159
(N.D. Ill. Nov. 10, 2010) 16, 17, 24, 25, 36

United States v. Leon,
468 U.S. 897 (1984) 25, 26, 46

United States v. Libby,
429 F. Supp. 2d 18 (D.D.C. 2008) 44

United States v. Marzook,
435 F. Supp. 2d 778 (N.D. Ill. 2006) 26

United States v. Medunjanin,
No. 10-CR-19-1, 2012 WL 526428
(S.D.N.Y. Feb. 16, 2012) 33, 41, 44

United States v. Megahey,
553 F. Supp. 1180 (E.D.N.Y. 1982) 17, 21, 41

United States v. Mubayyid,
521 F. Supp. 2d 125 (D. Mass. 2007) 26, 30, 32, 36, 46

United States v. Nicholson,
955 F. Supp. 588 (E.D. Va. 1997) 17, 39, 41

United States v. Nicholson,
No. 09-CR-40, 2010 WL 1641167 (D. Or. Apr. 21, 2010) 24, 43, 46

United States v. Ning Wen,
477 F.3d 896 (7th Cir. 2007) 25, 36, 46

United States v. Omar,
No. 13-2195, 2015 WL 3393825
(8th Cir. May 27, 2015) 23-24

United States v. Omar,
786 F.3d 1104 (8th Cir. 2015) 16, 17, 23

United States v. Ott,
827 F.2d 473 (9th Cir. 1987) 18-19, 21, 41, 42-43

United States v. Rahman,
861 F. Supp. 247 (S.D.N.Y. 1994), *aff'd*,
189 F.3d 88 (2d Cir. 1999) 12, 24, 29, 30, 35

United States v. Rosen,
447 F. Supp. 2d 538 (E.D. Va. 2006) 12, 24, 30, 45

United States v. Salameh,
152 F.3d 88 (2d Cir. 1998) 29-30

United States v. Sattar,
No. 02-CR-395, 2003 WL 22137012 (S.D.N.Y. 2003) 17

United States v. Sattar,
395 F. Supp. 2d 66 (S.D.N.Y. 2005) 35

United States v. Sherifi,
793 F. Supp. 2d 751 (E.D.N.C. 2011) 24

United States v. Spanjol,
720 F. Supp. 55 (E.D. Pa. 1989), *aff'd*,
958 F.2d 365 (3d Cir. 1992) 21, 45

United States v. Stewart,
590 F.3d 93 (2d Cir. 2009) 16, 17

United States v. Stone,
2011 WL 795104 (E.D. Mich.) 35

United States v. Thomson,
752 F. Supp. 75 (W.D.N.Y. 1990) 18, 30, 31

United States v. U.S. Gypsum Co.,
333 U.S. 364 (1948) 24

United States v. Warsame,
547 F. Supp. 2d 982 (D. Minn. 2008) 15, 24, 43, 45

United States v. Yunis,
867 F.2d 617 (D.C. Cir. 1989) 19

U.S. CONSTITUTION

Amend. I 12, 34, 35

Amend. IV 39

Amend. V 41

Amend. VI 39, 40

FEDERAL STATUTES

50 U.S.C. § 1801 ..... *passim*

50 U.S.C. §§ 1801-1812 1

50 U.S.C. § 1803 4

50 U.S.C. § 1804 ..... 5, 6, 8, 9

50 U.S.C. § 1805 ..... *passim*

50 U.S.C. § 1806 ..... 6, 14, 15, 22, 29, 40

50 U.S.C. § 1821 ..... *passim*

50 U.S.C. §§ 1821-1829 1

50 U.S.C. § 1823 ..... 5, 6, 8, 9

50 U.S.C. § 1824 ..... *passim*

50 U.S.C. § 1825 ..... *passim*

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("PATRIOT Act"), Pub. L. No. 107-56, 115 Stat. 272 (2001) 5

OTHER AUTHORITIES

H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., Pt. 1 (1978) 30, 31, 32-33

S. Rep. No. 95-701, 95th Cong., 2d Sess. (1978).....31, 32, 40-41

I. INTRODUCTION

The Government is filing this unclassified memorandum in opposition to the Defendant's Pretrial Motion to Suppress, and for the Disclosure of [Foreign Intelligence Surveillance Act (FISA)] Order, Application, and Related Materials (defendant's motion) (Def. Motion). The defendant seeks: (1) suppression of the evidence derived from FISA physical search(es) (*i.e.*, the FISA information); and, in the alternative, disclosure of the FISA application(s), order(s), and related materials (*i.e.*, the FISA materials). (Def. Motion, p. 2).[1]

The defendant has triggered this Court's review of the FISA materials related to the FISC-authorized physical search(es) to determine whether the FISA information was lawfully acquired and whether the physical search(es) was/were made in conformity with an order of authorization or approval.[2] Whenever "a motion is made pursuant to [50 U.S.C. § 1825(f)] . . . to discover or obtain applications or orders or other materials related to a physical search authorized by this title or to discover, obtain, or suppress evidence or information obtained or derived from a physical search . . . , the United States district court . . . shall . . . if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1825(g).

---

[1] **[CLASSIFIED MATERIAL REDACTED]**

[2] The provisions of FISA that address electronic surveillance generally are found at 50 U.S.C. §§ 1801-1812; those that address the physical search(es) at issue in this case are found at 50 U.S.C. §§ 1821-1829. These two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision.

The Government is filing herewith such an affidavit in which the Attorney General claims under oath that disclosure or an adversary hearing would harm the national security of the United States, which is the prerequisite for the Court to review the FISA materials *in camera* and *ex parte*;[3] consequently, the Government respectfully submits that, for the reasons set forth hereinafter, this Court should conduct an *in camera, ex parte* review of the documents relevant to the defendant's motion in accordance with the provisions of 50 U.S.C. § 1825(g).[4]

The Government respectfully submits that this Court will conclude from its *in camera, ex parte* review of the FISA materials that: (1) the physical search(es) at issue was/were both lawfully authorized and lawfully conducted in compliance with FISA; (2) disclosure to the defendant of the FISA materials and the Government's classified submissions is not authorized because the Court is able to make an accurate determination of the legality of the physical search(es) without disclosing the FISA materials or portions thereof; (3) the fruits of the physical search(es) should not be suppressed; (4) the defendant's motion should be denied to the extent that it seeks disclosure of FISA materials; and (5) no hearing is required.

A. BACKGROUND

On August 27, 2015, Gammal was charged by indictment in the Southern District of New York with one count each of: providing and attempting to provide material support to a foreign terrorist organization (FTO), in violation of 18 U.S.C. §§ 2339B and 2; conspiring to provide material support to an FTO, in violation of 18 U.S.C. § 2339B; aiding and abetting in the receipt

[3] The Attorney General's affidavit ("Declaration and Claim of Privilege") is filed both publicly and as an exhibit in the Sealed Appendix to this classified filing. *See* Sealed Exhibit 1.

[4] **[CLASSIFIED MATERIAL REDACTED]**

of military-style training from an FTO, in violation of 18 U.S.C. §§ 2339D and 2; and conspiracy to receive military-style training from an FTO, in violation of 18 U.S.C. § 371. (Doc. 3).

[CLASSIFIED MATERIAL REDACTED]

On July 13, 2016, pursuant to 50 U.S.C. § 1825(d), the United States provided notice to Gammal and this Court that it "intends to offer into evidence, or otherwise use or disclose . . . information obtained and derived from physical searches conducted pursuant to [FISA]." (Doc. 51). On August 12, 2016, Gammal filed his motion which seeks suppression of FISA information or, in the alternative, disclosure of FISA materials.

[CLASSIFIED MATERIAL REDACTED][5]

In subsequent sections of this Memorandum, the Government will: (1) present an overview of the FISA authorities at issue in this case; (2) discuss the FISA process; (3) address the manner in which the Court should conduct its *in camera, ex parte* review of the FISA materials; (4) summarize the facts supporting the FISC's probable cause determinations with respect to the target of the physical search(es) and to the facility(ies) targeted (all of which information is contained fully in the exhibits in the Sealed Appendix); (5) discuss the relevant minimization procedures; and (6) address the defendant's arguments in support of his motion. All of the Government's pleadings and supporting FISA materials are being submitted not only to oppose the defendant's motion, but also to support the United States' request, pursuant to FISA, that this Court: (1) conduct an *in camera, ex parte* review of the FISA materials; (2) find that the FISA information at issue was lawfully acquired and that the physical search(es) was/were conducted in conformity with an order of authorization or approval; (3) deny the

[5] As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

defendant's request that the FISA information be suppressed; and (4) order that none of the FISA materials be disclosed to the defense, and instead, that they be maintained by the United States under seal.

B. OVERVIEW OF THE FISA AUTHORITIES

[CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. The FISC's Findings

[CLASSIFIED MATERIAL REDACTED]

II. THE FISA PROCESS

A. OVERVIEW OF FISA[6]

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical searches when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court of Review ("FISC of Review"), which is composed of three United States District or Circuit Judges who are designated by the Chief Justice. 50 U.S.C. § 1803(b).

[6] This response references the statutory language in effect at the time relevant to this matter. Although only physical search(es) conducted pursuant to FISA are at issue in this matter, statutory language relating to such search(es) is closely tied to statutory language related to electronic surveillance. Accordingly, and for purposes of background only, the statutory requirements for both electronic surveillance and physical searches will be discussed in detail herein.

As originally enacted, FISA required that a high-ranking member of the Executive Branch of Government certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act").[7] One change to FISA accomplished by the USA PATRIOT Act is that a high-ranking official is now required to certify that the acquisition of foreign intelligence information is "a significant purpose" of the requested electronic surveillance or physical searches. 50 U.S.C. §§ 1804(a)(6)(B) and 1823(a)(6)(B).

FISA provides that the Attorney General may authorize the emergency employment of electronic surveillance and physical searches if the Attorney General

> (A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance [or physical search] to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;
>
> (B) reasonably determines that the factual basis for the issuance of an order under this title to approve such electronic surveillance [or physical search] exists;
>
> (C) informs, either personally or through a designee, a judge having jurisdiction under [50 U.S.C. § 1803] at the time of such authorization that the decision has been made to employ emergency electronic surveillance [or physical search]; and
>
> (D) makes an application in accordance with this title to a judge having jurisdiction under section 103 as soon as practicable, but not later than seven days after the Attorney General authorizes such electronic surveillance [or physical search].

[7] Pub. L. No. 107-56, 115 Stat. 272 (2001).

50 U.S.C. §§ 1805(e)(1) and 1824(e)(1).[8] Emergency electronic surveillance or physical searches must comport with FISA's minimization requirements, which are discussed below. *See* 50 U.S.C. §§ 1805(e)(2) and 1824(e)(2).[9]

B. THE FISA APPLICATION

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance, physical searches, or both, within the United States where a significant purpose is the collection of foreign intelligence information.[10] 50 U.S.C. §§ 1804(a)(6)(B) and 1823(a)(6)(B). Under FISA, "[f]oreign intelligence information" means:

> (1) information that relates to, and if concerning a United States person[11] is necessary to, the ability of the United States to protect against—
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

---

[8] **[CLASSIFIED MATERIAL REDACTED]**

[9] If no FISC order authorizing the electronic surveillance or physical searches is issued, emergency surveillance or searches must terminate when the information sought is obtained, when the FISC denies an application for an order, or after the expiration of seven days from the time of the emergency employment, whichever is earliest. *See* 50 U.S.C. §§ 1805(e)(3) and 1824(e)(3). Moreover, if no FISC order is issued, absent a showing of good cause, the FISC shall cause to be served on any U.S. person named in the application, and others in the FISC's discretion, notice of the fact of the application, the period of the surveillance, and the fact that during the period information was or was not obtained. *See* 50 U.S.C. §§ 1806(j) and 1824(j)(1). In addition, if no FISC order is issued, no information obtained or evidence derived from the emergency electronic surveillance or physical search may be disclosed in any court or other proceeding, and no information concerning a United States person acquired from the electronic surveillance or physical search may be used in any other manner by Federal officers or employees without the person's consent, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm. *See* 50 U.S.C. §§ 1805(e)(5) and 1824(e)(5).

[10] **[CLASSIFIED MATERIAL REDACTED]**

[11] **[CLASSIFIED MATERIAL REDACTED]**

> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to –
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e); *see also* 50 U.S.C. § 1821(1), adopting the definitions from 50 U.S.C. § 1801. With the exception of emergency authorizations, FISA requires that a court order be obtained before any electronic surveillance or physical searches may be conducted.

An application to conduct electronic surveillance pursuant to FISA must contain, among other things:

> (1) the identity of the federal officer making the application;
>
> (2) the identity, if known, or a description of the specific target of the electronic surveillance;
>
> (3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (4) a statement of the proposed minimization procedures to be followed;
>
> (5) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
>
> (6) a certification, discussed below, of a high-ranking official;
>
> (7) a summary of the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;

> (8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and
>
> (9) the proposed duration of the electronic surveillance.

50 U.S.C. §§ 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance except that an application to conduct a physical search must also contain a statement of the facts and circumstances that justify an applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that each "premises or property to be searched is or is about to be, owned, used, possessed by, or is in transit to or from" the target. 50 U.S.C. §§ 1823(a)(1)-(8), (a)(3)(B), and (C).

1. The Certification

An application to the FISC for a FISA order must include a certification from a high-ranking executive branch official with national security responsibilities that:

> (A) the certifying official deems the information sought to be foreign intelligence information;
>
> (B) a significant purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and
>
> (E) includes a statement of the basis for the certification that –
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6); *see also* 50 U.S.C. § 1823(a)(6).

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons obtained through FISA-authorized electronic surveillance or physical searches, including persons who are not the targets of the FISA authorities. FISA requires that such minimization procedures be "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1) and 1821(4)(A).

In addition, minimization procedures also include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. §§ 1801(h)(3) and 1821(4)(c).

[CLASSIFIED MATERIAL REDACTED]

3. Attorney General's Approval

FISA further requires that the Attorney General approve applications for electronic surveillance, physical searches, or both, before they are presented to the FISC.

C. THE FISC'S ORDERS

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance, physical searches, or both, only upon finding, among other things, that:

> (1) the application has been made by a "Federal officer" and has been approved by the Attorney General;
>
> (2) there is probable cause to believe that (A) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power (or that the premises or property to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power);
>
> (3) the proposed minimization procedures meet the statutory requirements set forth in 50 U.S.C. § 1801(h) (electronic surveillance) and 50 U.S.C. § 1821(4) (physical search);
>
> (4) the application contains all of the statements and certifications required by Section 1804 or Section 1823; and
>
> (5) if the target is a United States person, that the certifications are not clearly erroneous.

50 U.S.C. §§ 1805(a)(1)-(4) and 1824(a)(1)-(4).

> FISA defines "foreign power" to mean –
>
> (1) a foreign government or any component, thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> (4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

50 U.S.C. §§ 1801(a)(1)-(7); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"Agent of a foreign power" means –

(1) any person other than a United States person, who-

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4);

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore [sic];

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or

(2) any person who –

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence

> activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in [the subparagraphs above] . . . or knowingly conspires with any person to engage in activities described in [the subparagraphs above.]

50 U.S.C. §§ 1801(b)(1) and (2); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

FISA specifies that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. §§ 1805(a)(2)(A) and 1824(a)(2)(A). Although protected First Amendment activities cannot form the sole basis for FISA-authorized electronic surveillance or physical searches, they may be considered by the FISC if there is other activity indicative that the target is an agent of a foreign power. *See United States v. Rosen*, 447 F. Supp. 2d 538, 549-50 (E.D. Va. 2006) (if probable cause to believe target, "even if engaged in First Amendment activities, may also be involved in unlawful clandestine intelligence activities" or aiding and abetting such); *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999) (wrong to conclude that statements protected by the First Amendment could not be used to conclude one is an agent of a foreign power). Additionally, FISA provides that "[i]n determining whether or not probable cause exists . . . a judge may

consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b) and 1824(b).

If the FISC has made all of the necessary findings and is satisfied that the FISA application meets the statutory provisions, the FISC issues an *ex parte* order authorizing the electronic surveillance, physical searches, or both, requested in the application. 50 U.S.C. §§ 1805(a) and 1824(a). The order must specify:

> (1) the identity, if known, or a description of the specific target of the collection;
>
> (2) the nature and location of each facility or place at which the electronic surveillance will be directed or of each of the premises or properties that will be searched;
>
> (3) the type of information sought to be acquired and the type of communications or activities that are to be subjected to the electronic surveillance, or the type of information, material, or property that is to be seized, altered, or reproduced through the physical search;
>
> (4) the manner and means by which electronic surveillance will be effected and whether physical entry will be necessary to effect that surveillance, or a statement of the manner in which the physical search will be conducted;
>
> (5) the period of time during which electronic surveillance is approved and/or the authorized scope of each physical search; and
>
> (6) the applicable minimization procedures.

50 U.S.C. §§ 1805(c)(1) and (2)(A); 1824(c)(1) and (2)(A).

Under FISA, electronic surveillance or physical searches targeting a United States person may be approved for up to 90 days, and those targeting a non-United States person may be approved for up to 120 days. 50 U.S.C. §§ 1805(d)(1) and 1824(d)(1). Extensions may be granted, but only if the United States submits another application that complies with FISA's requirements. An extension for electronic surveillance or physical searches targeting a United

States person may be approved for up to 90 days, and one targeting a non-United States person may be approved for up to one year.[12] 50 U.S.C. §§ 1805(d)(2) and 1824(d)(2).

III. DISTRICT COURT REVIEW OF FISC ORDERS

FISA authorizes the use in a criminal prosecution of information obtained or derived from any FISA-authorized electronic surveillance or physical search, provided that advance authorization is obtained from the Attorney General, 50 U.S.C. §§ 1806(b) and 1825(c), and that proper notice is subsequently given to the court and to each aggrieved person against whom the information is to be used.[13] 50 U.S.C. §§ 1806(c)-(d) and 1825(d)-(e). Upon receiving notice, an aggrieved person against whom the information is to be used may move to suppress the use of the FISA information on two grounds: (1) that the information was unlawfully acquired; or (2) that the electronic surveillance or physical search was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e) and 1825(f). In addition, FISA contemplates that a defendant may file a motion or request under any other statute or rule of the United States to discover or obtain applications or orders or other materials relating to electronic surveillance or physical searches, *i.e.*, the FISA materials, 50 U.S.C. §§ 1806(f) and 1825(g). When a defendant moves to suppress FISA information under 50 U.S.C. §§ 1806(e) or 1825(f), or seeks to discover the FISA materials under some other statute or rule, the motion or request is

---

[12] The FISC retains the authority to review, before the end of the authorized period of electronic surveillance or physical searches, the Government's compliance with the requisite minimization procedures. 50 U.S.C. §§ 1805(d)(3) and 1824(d)(3).

[13] An "aggrieved person" is defined as "a person whose premises, property, information, or material is the target of physical search" or "whose premises, property, information, or material was subject to physical search." 50 U.S.C. § 1821(2). Gammal is an "aggrieved person" under Title III of FISA and, as noted above, he was provided with notice of his status as such and of the Government's intent to use FISA-obtained or -derived information against him at trial.

evaluated using FISA's probable cause standard, which is discussed below, and not the probable cause standard applicable to criminal warrants. *See, e.g.*, *United States v. El-Mezain*, 664 F.3d 467, 564 (5th Cir. 2011) ("[R]ather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power."); *United States v. Duka*, 671 F.3d 329, 336-37 (3d Cir. 2011) (rejecting appellant's challenge to FISA's probable cause standard because it does not require any indication that a crime has been committed).

A. THE REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

In assessing the legality of FISA-authorized electronic surveillance and physical searches, or both, the district court,

> shall, notwithstanding any other law, if the Attorney General files an affidavit or declaration under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.[14]

50 U.S.C. §§ 1806(f) and 1825(g). On the filing of the Attorney General's affidavit or declaration (which accompanies this response), the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance [or physical search] only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]."[15] 50 U.S.C. §§ 1806(f) and 1825(g). Thus, the propriety of the disclosure of any FISA applications or

---

[14] **[CLASSIFIED MATERIAL REDACTED]**

[15] In *United States v. Warsame*, 547 F. Supp. 2d 982, 987 (D. Minn. 2008), the court addressed the meaning of "necessary" in this context: "[t]he legislative history explains that such disclosure is 'necessary' only where the court's initial review indicates that the question of legality may be complicated" by factual misrepresentations, insufficient identification of the target, or failure to comply with the minimization standards in the order.

orders to a defendant may not even be considered unless and until the district court has first concluded that it is unable to make an accurate determination of the legality of the acquired collection after reviewing the Government's submissions (and any supplemental pleadings that the district court may request) *in camera* and *ex parte*. *See United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010) (disclosure of FISA materials "is the exception and *ex parte*, *in camera* determination is the rule") (quoting *United States v. Stewart*, 590 F.3d 93, 129 (2d Cir. 2009)); *United States v. Omar*, 786 F.3d 1104, 1110 (8th Cir. 2015) ("[D]isclosure and an adversary hearing are the exception occurring *only* when necessary.") (emphasis in original) (quoting *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991), which in turn quoted *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982)); *El-Mezain*, 664 F.3d at 565 (quoting 50 U.S.C. § 1806(f) and emphasizing the word "necessary").

If the district court is able to make an accurate determination of the legality of the electronic surveillance, physical searches, or both, based on its *in camera*, *ex parte* review of the materials submitted by the United States, then the court *may not* order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. *El-Mezain*, 664 F.3d at 566; *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984); *United States v. Kashmiri*, No. 09-CR-830, 2010 WL 4705159, at *2-3 (N.D. Ill. Nov. 10, 2010).

1. *In Camera, Ex Parte* Review is the Rule

Federal courts have repeatedly and consistently held that FISA anticipates an "*ex parte*, *in camera* determination is to be the rule," *Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (*quoting Belfield*, 692 F.2d at 147), with disclosure and an adversarial hearing being the "exception, occurring *only* when necessary." *Omar*, 786 F.3d at 1110. In fact, every court but one (whose

decision was subsequently overturned by an appellate court)[16] that has addressed a motion to disclose FISA materials or to suppress FISA information has been able to reach a conclusion as to the legality of the FISA collection at issue based on its *in camera, ex parte* review. *See, e.g.*, *Stewart*, 590 F.3d at 128 (quoting *Belfield*, 692 F.2d at 147 that "*ex parte, in camera* determination is to be the rule"); *United States v. Sattar*, No. 02-CR-395, 2003 WL 22137012, at *6 (S.D.N.Y. 2003) (citing *United States v. Nicholson*, 955 F. Supp. 588, 592 & n. 11 (E.D. Va. 1997)) (noting "this court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance"); *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310 (D. Conn. 2008), *aff'd*, 630 F.3d 102, 129 (2d Cir. 2010) ("Courts have uniformly held that *ex parte* and *in camera* inspections are the 'rule' under FISA"); *Kashmiri*, 2010 WL 4705159, at *2-3 ("the procedure a district court follows in such a situation is an *ex parte* and *in camera* review" as explained in *Duggan*, 743 F.2d at 78); *United States v. Megahey*, 553 F. Supp. 1180, 1193 (E.D.N.Y. 1982), *aff'd without opinion*, 729 F.2d 1444 (2d Cir. 1983), *aff'd sub nom. Duggan*, 743 F.2d at 74) ("the legality of electronic surveillance can be determined on an *ex parte, in camera* basis"); *Omar*, 786 F.3d at 1111; *Isa*, 923 F.2d at 1306 (the Court's "study of the materials leaves no doubt that substantial national security interests required the *in camera, ex parte* review, and that the district court properly conducted such a review"); *El-Mezain*, 664 F.3d at 566-67 (quoting district court's statement that no court has ever held an adversarial hearing to assist the court); *In re Grand Jury Proceedings*

[16] The district court in *United States v. Daoud*, 2014 WL 321384 (N.D. Ill. 2014), ruled that it was capable of making the determination, but nevertheless ordered the disclosure of FISA materials. The Government appealed the *Daoud* court's order to the U.S. Court of Appeals for the Seventh Circuit, which overturned the district court's decision to disclose, stating, "[s]o clear is it that the materials were properly withheld from defense counsel that there is no need for a remand to enable the district judge to come to the same conclusion, because she would have to do so." *Daoud*, 755 F.3d 479, 485 (7th Cir. 2014).

of the Special Apr. 2002 Grand Jury ("*In re Grand Jury Proceedings*"), 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court had ever ordered disclosure of FISA materials); *United States v. Thomson*, 752 F. Supp. 75, 77 (W.D.N.Y. 1990) ("the Court must conduct an *ex parte, in camera* review").

As the exhibits in the Sealed Appendix make clear, there is nothing extraordinary about the instant FISA-authorized physical search(es) that would justify the production and disclosure of highly sensitive and classified FISA materials or the suppression of FISA-obtained or -derived evidence. Here, the FISA materials are well-organized and easily reviewable by the Court *in camera* and *ex parte*, and they are fully and facially sufficient to allow the Court to make an accurate determination that the FISA information was lawfully acquired and that the physical search(es) was/were made in conformity with an order of authorization or approval. In other words, the materials presented "are straightforward and readily understood." *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986). Moreover, as in other cases, "Court review of the FISA materials in this case is relatively straightforward and not complex." *Abu-Jihaad*, 531 F. Supp. 2d at 310. *See also Thomson*, 752 F. Supp. at 79 ("the Court finds that the issues in this case are not so complex that the participation of the defendant is required to accurately determine the legality of the surveillance at issue."). This Court, much like the others, is capable of reviewing the FISA materials *in camera* and *ex parte* and making the requisite legal determination without an adversarial hearing.

In addition to the specific harm that would result from the disclosure of the FISA materials in this case, which is detailed in the classified declaration of a high-ranking FBI official in support of the Attorney General's Declaration and Claim of Privilege, the underlying rationale for non-disclosure is clear: "In the sensitive area of foreign intelligence gathering, the need for

extreme caution and sometimes even secrecy may not be overemphasized." *United States v. Ott*, 827 F.2d 473, 477 (9th Cir. 1987) ("Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to *anyone* not involved in the surveillance operation in question.") (emphasis in original); *accord United States v. Islamic Am. Relief Agency ("IARA")*, No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *3-4 (W.D. Mo. Dec. 21, 2009).

Confidentiality is critical to national security. "If potentially valuable intelligence sources" believe that the United States "will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information." *Central Intelligence Agency v. Sims*, 471 U.S. 159, 175 (1985); *see also Phillippi v. Central Intelligence Agency*, 655 F.2d 1325, 1332-33 (D.C. Cir. 1981) (discussing import of national security in the context of Freedom of Information Act request). When considering whether the disclosure of classified sources, methods, techniques, or information would harm the national security, federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of weighing a variety of subtle and complex factors in determining whether the disclosure of information may lead to an unacceptable risk of compromising the intelligence gathering process, and determining whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of information that, when revealed, could reasonably be expected to harm the national security of the United States. *See Sims*, 471 U.S. at 180; *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."); *Halperin v. Central Intelligence Agency*, 629

F.2d 144, 150 (D.C. Cir. 1980) ("each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself"). An adversary hearing is not only unnecessary to aid the Court in the straightforward task before it, but such a hearing would also create potential dangers that courts have consistently sought to avoid.

As the *Belfield* court explained:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law enforcement surveillance.

692 F.2d at 148 (footnotes and citations omitted); *see also ACLU Found. of So. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) (citing *Belfield* for the proposition that *ex parte* and *in camera* review "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance").

2. *In Camera, Ex Parte* Review is Constitutional

Numerous cases support the conclusion that the legality of FISA physical searches and electronic surveillance should be determined on an *in camera, ex parte* basis. *Abu-Jihaad*, 630 F.3d at 129 (affirmed district court's determination that "its *in camera, ex parte* review permitted it to assess the legality of the challenged surveillance and the requirements of due process did not counsel otherwise."); *Isa*, 923 F.2d at 1306 (upholding the district court's *in camera, ex parte* review as constitutional and stating that the process delineated under FISA "provides even more

protection" than defendants receive in other contexts); *El-Mezain*, 664 F.3d at 567 (agreeing with district court that its *in camera, ex parte* review ensured the defendant's constitutional and statutory rights were not violated); *United States v. Spanjol*, 720 F. Supp. 55, 58-59 (E.D. Pa. 1989), *aff'd*, 958 F.2d 365 (3d Cir. 1992), (this procedure uniformly followed by other courts); *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005) ("FISA's requirement that the district court conduct an *ex parte*, *in camera* review of FISA materials does not deprive a defendant of due process."); *Ott*, 827 F.2d at 476-77 (FISA's review procedures do not deprive a defendant of due process); *United States v. Gowadia*, No. 05-00486, 2009 WL 1649714, at *2 (D. Hawaii 2009) ("courts have uniformly held that the in camera review procedures prescribed by FISA do not deprive a defendant of Due Process under the United States Constitution."); *United States v. Jayyousi*, No. 04-60001, 2007 WL 851278, at *7-8 (S.D. Fla. Mara. 15, 2007) ("FISA procedures do not violate Defendant's due process rights.");[17] *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. 2006) (previously addressed and rejected Fifth Amendment right to due process and Sixth Amendment right to counsel claims); *ACLU Found.*, 952 F.2d at 465 (procedure under FISA "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance."); *Megahey*, 553 F. Supp. at 1194 ("*ex parte*, *in camera* procedures provided in [FISA] are constitutionally sufficient to determine the lawfulness of the electronic surveillance at issue while safeguarding defendant's fourth amendment rights").

In summary, FISA mandates a process by which the district court must conduct an initial *in camera, ex parte* review of FISA applications, orders, and related materials to determine

[17] All citations to *Jayyousi* herein are to the Magistrate Judge's Report and Recommendation, which was adopted and incorporated into the Court's Opinion.

whether the FISA information was lawfully acquired and whether the electronic surveillance and physical searches were made in conformity with an order of authorization or approval. Such *in camera, ex parte* review is the rule in such cases and that procedure is constitutional. In this case, the Attorney General has filed the required declaration invoking that procedure and has declared that disclosure or an adversary hearing would harm national security. Accordingly, an *in camera, ex parte* review by this Court is the appropriate venue to determine whether the FISA information was lawfully acquired and whether the physical search(es) was/were made in conformity with an order of authorization or approval.

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

1. Standard of Review of Probable Cause

In evaluating the legality of the FISA collection, the district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause showing required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31; *see also* 50 U.S.C. §§ 1806(f) and 1825(g).

Although federal courts are not in agreement as to whether the probable cause determination at the FISC should be reviewed *de novo* or accorded due deference, the Second Circuit has previously afforded due deference to the determination of the FISC. *Abu-Jihaad*, 630 F.3d at 130 ("Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submissions in this case would easily allow it to clear a higher standard of review."); *accord United States v. Ahmed*, No. 1:06-CR-147, 2009 U.S. Dist. Lexis 120007 at *21-22 (N.D. Ga. Mar. 19, 2009) (citing *Illinois v. Gates*, 462 U.S. at 236) (FISC's "determination of probable cause should be given 'great deference' by the

reviewing court"). The material under review here satisfies either standard of review. *See Omar*, 786 F.3d at 1112 ("[W]e have no hesitation in concluding that probable cause under FISA existed under any standard of review.") [18]

2. Probable Cause Standard

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, or that the property or premises to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power. It is this standard—not the standard applicable to criminal search warrants—that this Court must apply. *See Abu-Jihaad*, 630 F.3d at 130-31; *El-Mezain*, 664 F.3d at 564 ("[t]his probable cause standard is different from the standard in the typical criminal case because, rather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power"); *Duka*, 671 F.3d at 338; *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (citing *United States v. United States District Court (Keith)*, 407 U.S. 297, 322 (1972)).

[CLASSIFIED MATERIAL REDACTED]

3. Standard of Review of Certifications

Certifications submitted in support of a FISA application should be "subjected to only minimal scrutiny by the courts," and are "presumed valid." *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008) (quoting *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987)); *United States v. Omar*, Cr. No. 09-242, 2012 WL 2357734, at *3 (D. Minn. 2012) ("FISA warrants are

[18] **[CLASSIFIED MATERIAL REDACTED]**

subject to 'minimal scrutiny by the courts,' both upon initial presentation and subsequent challenge" and that "the reviewing court must presume as valid 'the representations and certifications' . . . "); *Warsame*, 547 F. Supp. 2d at 990 ("a presumption of validity [is] accorded to the certifications"); *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011) ("presumption of validity accorded to the certifications"); *United States v. Nicholson*, No. 09-CR-40, 2010 WL 1641167, at *5 (D. Or. 2010) ("certifications contained in applications for FISA surveillance orders are 'presumed valid.'" (quoting *Rosen*, 447 F. Supp. 2d at 545)). When a FISA application is presented to the FISC, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77. Likewise, Congress intended that the reviewing district court should "have no greater authority to second-guess the executive branch's certifications than has the FISA judge." *Id.*; *see also Rahman*, 861 F. Supp. at 250 (not the function of the "judge to 'second-guess' the certifications."); *In re Grand Jury Proceedings*, 347 F.3d at 204-05 (same); *Badia*, 827 F.2d at 1463 (minimal scrutiny); *IARA*, 2009 WL 5169536, at *4 (same); *Kashmiri*, 2010 WL 4705159, at *1 (same).

The district court's review should determine whether the certifications were made in accordance with FISA's requirements. *See Duggan*, 743 F.2d at 77 ("a reviewing court is to have no greater authority to second-guess the executive branch's certifications than has the FISA Judge . . . ."); *Omar*, 2012 WL 2357734, at *3 ("The reviewing court must presume as valid 'the representations and certifications submitted in support of an application for FISA surveillance' . . . absent a showing sufficient to trigger a *Franks* hearing"); *see also Campa*, 529 F.3d at 993 ("In the absence of a *prima facie* showing of a fraudulent statement by the certifying officer, procedural regularity is the only determination to be made if a non-United States person is the

target") (quoting *Badia*, 827 F.2d at 1463). When the target is a United States person, then the district court should also ensure that each certification is not "clearly erroneous."[19] *Duggan*, 743 F.2d at 77; *Campa*, 529 F.3d at 994; *Kashmiri*, 2010 WL 4705159, at *2. A "clearly erroneous" finding is established only when "the reviewing court on the [basis of the] entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); *United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005) (quoting *U.S. Gypsum Co.*, 333 U.S. at 395); *IARA*, 2009 WL 5169536, at *4 (identifying "clearly erroneous" standard of review for FISA certifications).

4. FISA Is Subject to the "Good-Faith" Exception

Even assuming *arguendo* that this Court determines that a particular FISC order was not supported by probable cause, or that one or more of the FISA certification requirements were not in fact met, the evidence obtained or derived from the FISA-authorized physical search(es) is, nonetheless, admissible under the "good faith" exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984).[20] The Seventh Circuit, relying on *Leon*, has stated that federal officers were entitled to rely in good faith on a FISA warrant. *United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007). As the court noted:

> [T]he exclusionary rule must not be applied to evidence seized on the authority of a warrant, even if the warrant turns out to be defective, unless the affidavit supporting the warrant was false or misleading, or probable cause was so transparently missing that "no reasonably well trained officer [would] rely on the warrant."

---

[19] **[CLASSIFIED MATERIAL REDACTED]**

[20] "[E]ven if we were to conclude that amended FISA is unconstitutional, evidence derived from it would nevertheless have been admissible in the government's case. . . . [t]he exclusionary rule precludes the admission of evidence tainted by a Fourth Amendment violation" only in those cases where its application will deter police misconduct. *Duka*, 671 F.3d at 346 (citing *Leon*, 468 U.S. at 918).

Id. (quoting *Leon*) (alteration in original); *see also Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8, 26-27 ("The FISA evidence obtained . . . would be admissible under *Leon*'s 'good faith' exception to the exclusionary rule were it not otherwise admissible under a valid warrant."); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 140 n. 12 (D. Mass. 2007) (applying the exception because "there appears to be no issue as to whether the government proceeded in good faith and in reasonable reliance on FISA orders"); *United States v. Marzook*, 435 F. Supp. 2d 778, 790-91 (N.D. Ill. 2006) (holding, in an analogous context, that "the FBI's reliance on the Attorney General's approval under Executive Order No. 12333 - an order that no court has found unconstitutional - was [] objectively reasonable because that order pertains to foreign intelligence gathering.").

The FISA-authorized physical search(es) at issue in this case would fall squarely within this "good-faith exception." There is no basis to find that any declarations or certifications at issue in this case were deliberately or recklessly false. *See Leon*, 468 U.S. at 914-15; *see also Massachusetts v. Sheppard*, 468 U.S. 981 (1984) (exclusionary rule not applicable when officers conduct search in objectively reasonable reliance on a warrant). Further, there are no facts indicating the FISC failed to act in a neutral and detached manner in authorizing the physical search(es) at issue. *Leon*, 468 U.S. at 914-15. Moreover, as the Court will see from its *in camera, ex parte* review of the FISA materials, facts establishing the requisite probable cause were submitted to the FISC, the FISC's orders contained all of the requisite findings, and "well-trained officers" reasonably relied on those orders. Therefore, if the Court questions whether a particular FISC order was supported by sufficient probable cause, the information obtained pursuant to those orders would be admissible under *Leon*'s "good faith" exception to the exclusionary rule.

IV. THE FISA INFORMATION WAS LAWFULLY ACQUIRED AND THE PHYSICAL SEARCH(ES) WERE MADE IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED MATERIAL REDACTED]

A. THE INSTANT FISA APPLICATION(S) MET FISA'S PROBABLE CAUSE STANDARD

[CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

c. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

d. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

e. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

B. THE CERTIFICATIONS COMPLIED WITH FISA

[CLASSIFIED MATERIAL REDACTED]

1. Foreign Intelligence Information

[CLASSIFIED MATERIAL REDACTED]

2. "A Significant Purpose"

[CLASSIFIED MATERIAL REDACTED]

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED MATERIAL REDACTED]

For all of the above reasons, the FISC correctly found that the certifications were not clearly erroneous.

C. THE PHYSICAL SEARCH(ES) WAS/WERE CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

This Court's *in camera, ex parte* review of the FISA materials will demonstrate not only that the FISA information was lawfully acquired, but also that the physical search(es) was/were lawfully conducted. That is, the FISA-obtained or -derived information that will be offered into evidence in this case was acquired, retained, and disseminated by the FBI in accordance with FISA's minimization requirements, and the standard minimization procedures ("SMPs") adopted by the Attorney General and approved by the FISC.

1. The Standard Minimization Procedures

In accordance with the SMPs in effect at the time the physical search(es) occurred, once a reviewing court is satisfied that the electronic surveillance or physical searches were properly certified and the information was lawfully acquired pursuant to FISA, it must then examine

whether the electronic surveillance or physical searches were lawfully conducted. *See* 50 U.S.C. §§ 1806(e)(2), 1825(f)(1)(B). In order to examine whether the electronic surveillance or physical searches were lawfully conducted, the reviewing court must determine whether the Government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

[CLASSIFIED MATERIAL REDACTED]

FISA's legislative history and the applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into account the realities of collecting foreign intelligence because the activities of persons engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. *See Rahman*, 861 F. Supp. at 252-53. The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d 717, 741 (Foreign Int. Surv. Ct. of Rev. 2002); *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 286 (S.D.N.Y. 2000) ("more extensive monitoring and greater leeway in minimization efforts are permitted in a case like this given the world-wide, covert and diffuse nature of the international terrorist group(s) targeted" [internal quotation marks omitted]). Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities and other practices designed to conceal the breadth and aim of their operations, organization, activities and plans. *See, e.g., United*

States v. Salameh, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *Kevork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., Pt. 1, at 55 (1978) (hereinafter "House Report")); *see also United States v. Hammoud*, 381 F.3d 316, 334 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005) (citing *Salameh*, 152 F.3d at 154); *In re Sealed Case*, 310 F.3d at 740-41; *Thomson*, 752 F. Supp. at 81 (noting that it is permissible to retain and disseminate "bits and pieces" of information until the information's "full significance becomes apparent") (citing House Report, part 1, at 58); *Bin Laden*, 126 F. Supp. 2d at 286. Likewise, "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." *Rahman*, 861 F. Supp. at 252-53 (citing House Report, part 1, at 55, 59). The Government must be given flexibility where the conversations are carried out in a foreign language. *Mubayyid*, 521 F. Supp. 2d at 134; *Rahman*, 861 F. Supp. at 252. As a result, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power. As Congress explained:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

House Report, part 1, at 58. Indeed, at least one court has cautioned that, when a U.S. person communicates with an agent of a foreign power, the Government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *Thomson*, 752 F. Supp. at 82.

Congress also recognized that agents of a foreign power are often very sophisticated and skilled at hiding their activities. *Cf. Thomson*, 752 F. Supp. at 81 (quoting House Report part 1, at 58). Accordingly, to pursue leads, Congress intended that the Government be given "a significant degree of latitude" with respect to the "retention of information and the dissemination of information between and among counterintelligence components of the Government." *Cf. Id.*

In light of these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. Rep. No. 95-701, 95th Cong., 2d Sess., 39 (quoting *Keith*, 407 U.S. at 323) (1978) ("Senate Report"). The Fourth Circuit reached the same conclusion in *Hammoud*, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance." 381 F.3d at 334.

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with

respect to particular communications. Rather, as the United States Supreme Court stated in the context of Title III surveillance, there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." *Scott v. United States*, 436 U.S. 128, 136 (1978). "The test of compliance is 'whether a good-faith effort to minimize was made.'" *Mubayyid*, 521 F. Supp. 2d at 135; *see also Hammoud*, 381 F.3d at 334 ("[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information"); *see also* Senate Report at 39-40 (stating that the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion"); *IARA*, 2009 WL 5169536, at *6 (quoting Senate Report at 39-40).

Moreover, as noted above, FISA expressly states that the Government is not required to minimize information that is "evidence of a crime," whether or not it is also foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); *see also Isa*, 923 F.2d at 1304 (noting that "[t]here is no requirement that the 'crime' be related to foreign intelligence"). As a result, to the extent that certain communications of a United States person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See Id* at 1305.

Even assuming, *arguendo*, that certain communications were not properly minimized, suppression would not be the appropriate remedy with respect to those communications that met the standard. *Cf. United States v. Falcone*, 364 F. Supp. 877, 886-87 (D.N.J. 1973), *aff'd*, 500 F.2d 1401 (3d Cir. 1974) (Title III). As discussed above, absent evidence that "on the whole" there has been a "complete" disregard for the minimization procedures, the fact that some communications should have been minimized does not affect the admissibility of others that

were properly acquired and retained. Indeed, Congress specifically intended that the only evidence that should be suppressed is the "evidence which was obtained unlawfully." House Report at 93. FISA's legislative history reflects that Congress intended only a limited sanction for errors of minimization:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

Id.; *see also Falcone*, 364 F. Supp. at 886-87; *accord, United States v. Medunjanin*, No. 10-CR-19-1, 2012 WL 526428, at *12 (E.D.N.Y. 2012) (disclosure and suppression not warranted where "failure to adhere to [the minimization] protocol was *de minimis*").

2. The FISA Information Was Appropriately Minimized

[CLASSIFIED MATERIAL REDACTED]

Based upon this information, the Government respectfully submits that it lawfully conducted the FISA collection(s) discussed herein. Consequently, for the reasons stated above, the Court should find that the FISA collection(s) discussed herein was/were lawfully conducted under the minimization procedures approved by the FISC and applicable to the FISA collections discussed herein.

V. THE COURT SHOULD REJECT THE DEFENDANT'S LEGAL ARGUMENTS

In his motion, the defendant requests that the Court order the suppression of the evidence derived from FISA search(es) or, in the alternative, order the disclosure of the FISA application(s), order(s), and related materials (Def. Motion, p. 2). The Government disputes the

defendant's legal and factual assertions regarding the disclosure of the FISA materials and the suppression of the FISA information and will address each of his arguments in turn below.

A. THE FISA INFORMATION SHOULD NOT BE SUPPRESSED

In support of his argument to suppress the FISA information (*i.e.*, the information obtained or derived from the FISC-authorized physical search(es)), the defendant asserts that: (1) the Government could not have shown Gammal was an agent of a foreign power (Def. Motion, pp. 7-8); (2) the FISC's probable cause determination may have been predicated solely on activities protected by the First Amendment (Def. Motion, pp. 8-10); (3) a significant purpose of the physical search(es) was not to gather foreign intelligence information (Def. Motion, p. 10); (4) the FISA materials may contain intentionally or recklessly false statements or material omissions (Def. Motion, pp. 11-14); (5) the certifications required by FISA may have not been contained in the application(s) made to the FISC (Def. Motion, pp. 14); and (6) the Government may not have properly minimized the FISA information (Def. Motion, pp.14-16).

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. The FISA Application(s) Was/Were Not Based Solely on Protected First Amendment Activity

The defendant claims that "[t]he FBI placed heavy emphasis on El Gammal's political views in securing its first search warrant for his Facebook account" and speculates that "[t]he government may have done the same in its FISA application." (Def. Motion, pp. 9-10). Not all speech- or advocacy-related activities fall within the protection of the First Amendment. For instance, conversations with co-conspirators merit no First Amendment protection because they are statements made in furtherance of a conspiracy and are evidence of the participant's criminal intent. "Numerous crimes under the federal criminal code are, or can be, committed by speech

alone . . . . [I]f the evidence shows that the speech crossed the line into criminal solicitation, procurement of criminal activity, or conspiracy to violate the laws, the prosecution is permissible." *Rahman*, 189 F.3d at 117; *United States v. Sattar*, 395 F. Supp. 2d 79, 101 (S.D.N.Y. 2005) ("First Amendment lends no protection to participation in conspiracy, even if such participation is through speech"); *United States v. Stone*, 2011 WL 795104, at *10 (E.D. Mich. January 12, 2011) (defendants not charged with advocacy, but "[r]ather they are charged with an actual agreement to commit actual acts").

[CLASSIFIED MATERIAL REDACTED]

3. A Significant Purpose of the FISA Physical Search(es) Was the Collection of Foreign Intelligence Information and the Certifications Complied with FISA

The defendant states that if "the purpose of the FISA search of El Gammal's Facebook account was to gather evidence of his past criminal activity [then] the search was unlawful." (Def. Motion, p. 10). The defendant further requests that the Court "review the FISA applications to determine whether they contain the certifications required by [FISA]." (Def. Motion, p. 14).

[CLASSIFIED MATERIAL REDACTED]

4. The Defendant Has Not Established Any Basis for the Court to Conduct a *Franks* Hearing

The defendant notes that "[t]he Fourth Amendment limits the use of evidence derived from a warrant tainted by misinformation" and claims that the "possibility that the government has submitted FISA applications with intentionally or recklessly false statements or material omissions is not speculative." (Def. Motion, p. 11). The defendant cites to misstatements of fact he claims exist in criminal search warrants related to Gammal. (Def. Motion, p. 13). To the extent the defendant intends to argue that he is entitled to a *Franks* hearing based on purported

misrepresentations or material falsehoods in the FISA application(s) in this case, the Court should deny this request.

When a defendant makes the requisite showing, the Court may conduct a *Franks* hearing to determine if there are material misrepresentations of fact, or omissions of material fact, before the FISC sufficient to warrant suppression of evidence obtained or derived from Title I and Title III FISA collections. *See Franks*, 438 U.S. at 171; *Ning Wen*, 477 F.3d at 897. To merit a *Franks* hearing, the defendant first must make a "concrete and substantial preliminary showing" that: (1) the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit; and (2) the misrepresentation was essential to the finding of probable cause. *Franks*, 438 U.S. at 155-56; *Duggan*, 743 F.2d at 77 & n.6; *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990); *Kashmiri*, 2010 WL 4705159 at *5 (defendant "has not made any showing – let alone a substantial one – that an Executive Branch officer knowingly and intentionally, or recklessly, included a false statement in the FISA application [and w]ithout such a showing, he is foreclosed from obtaining a hearing"). Failure of the defendant "to satisfy either of these two prongs proves fatal to a *Franks* hearing." *Id.* at *5; *Mubayyid*, 521 F. Supp. 2d at 130-31.

The defendant claims that a *Franks* hearing "may be appropriate in order to allow the defense the opportunity to prove that the affiants before the FISA Court intentionally or recklessly made materially false statements and omitted material information from the FISA applications." (Def. Motion, at 13). This approach would allow him, and defendants in every case, to obtain the FISA materials merely by alleging some impropriety.[21] Disclosing FISA

[21] One court referred to this as "backward reasoning" in denying a defendant's motion to suppress FISA-derived evidence. *United States v. Mihalik*, 11-CR-833(A), Doc. 108, at 2 (C.D. Cal. 2012) (Minute Order Denying Defendant's Motion to Suppress FISA-Derived Evidence).

materials to defendants would then become the rule, violating Congress' clear intention, set forth in 50 U.S.C. § 1825(g), that the FISA materials be reviewed *ex parte* and *in camera* in a manner consistent with the realities of modern intelligence needs and investigative techniques. Courts have acknowledged that the FISA statute does not envision such disclosure without establishing a basis for it.

The standard for a *Franks* hearing is a high one. *Rivera v. United States*, 928 F.2d 592, 604 (2d Cir. 1991). The defendant must submit allegations of deliberate falsehood or of reckless disregard for the truth, accompanied by an offer of proof. *Franks*, 438 U.S. at 171. Allegations of negligence or innocent mistake are insufficient, *id.*, as are allegations of insignificant or immaterial misrepresentations or omissions. *Colkley*, 899 F.2d at 301-02. Moreover, a defendant's lack of access to the FISA applications and orders is not an adequate substitute for the required showing. Although this situation presents a challenge for defense counsel, Congress and the courts have recognized that such difficulty does not justify the disclosure of FISA materials. In *Belfield*, for example, the court noted that "Congress was also aware of these difficulties [faced by defense counsel without access to FISA materials and] chose to resolve them through means other than mandatory disclosure." *Belfield*, 692 F.2d at 148. The Court found that the defendant's "claim of complexity can be given no concreteness. It is pure assertion." *Id.*

[CLASSIFIED MATERIAL REDACTED][22]

---

[22] The defendant also cites a 2006 report by the U.S. Department of Justice Inspector General (IG) that reviewed the FBI's record of compliance with FISA orders, investigative guidelines promulgated by the Attorney General, and guidelines on the use of National Security Letters. (Def. Motion, p. 12). However, the IG's report is silent on the point for which the defendant cites it: it does *not* address the accuracy of applications submitted to the FISC.

In sum, the defendant has failed to carry this burden of establishing the prerequisites for a *Franks* hearing, and there is no basis to support holding a *Franks* hearing. For these reasons, the Court should deny any defense request for a *Franks* hearing and his request for disclosure of the FISA materials.

5. The Government Complied with the Minimization Procedures

[CLASSIFIED MATERIAL REDACTED]

As the Court will see from its *ex parte*, *in camera* review of the FISA materials, the Government complied with all of FISA's statutory requirements. Accordingly, the Government submits that there is no basis to suppress the FISA information in the present case.

B. THERE SHOULD BE NO DISCLOSURE OF FISA MATERIALS TO THE DEFENDANT OR HIS COUNSEL

In support of his argument to disclose the FISA materials (*i.e.*, the application(s), order(s), and other materials relating to the physical search(es)), the defendant asserts that the Court must do so because: (1) the defense has a "constitutional entitlement" to disclosure under the Fourth, Fifth and Sixth Amendments (Def. Motion, pp. 17-18); (2) it is "impossible" for the Court to accurately determine the legality of the physical search(es) without the assistance of defense counsel (Def. Motion, pp. 17); and (3) defense counsel has appropriate security clearances and can be trusted to hold secret information in confidence (Def. Motion, pp. 17). As discussed below, Congress's clear intention is that FISA materials should be reviewed *in camera* and *ex parte*, and in a manner consistent with the realities of modern intelligence needs and investigative techniques. Indeed, this Court will find upon its own review that there is nothing extraordinary about this case that would prompt this Court to order disclosure and that the defendant has failed to present any colorable basis for the Court to order disclosure of the FISA materials.

1. Due Process Does Not Require Disclosure

The defendant states that "*ex parte* proceedings impair the integrity of the adversary process and the criminal justice system," citing to the Fifth and Sixth Amendments (Def. Motion, p. 17), and do not "provide the scrutiny that the Fourth Amendment exclusionary rule demands." (Def. Motion, pp. 18-19, *quoting Alderman v. United States*, 394 U.S. 165, 184 (1969)). The defendant's claims are contrary to all of the relevant case law (as opposed to the case law cited by the defense, which does not address FISA). Several courts have found FISA's *in camera* review provisions to be constitutional. *Duggan*, 743 F.2d at 73 ("[w]e regard the procedures fashioned in FISA as a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information."); *Abu-Jihaad*, 630 F3d. at 143 (FISA "strikes a reasonable balance between the government's interest in obtaining foreign intelligence information and the protection of individuals' Fourth Amendment rights."); *United States v. Falvey*, 540 F. Supp. 1306, 1315-16 (E.D.N.Y. 1982) (rejecting First, Fifth, and Sixth Amendment challenges and noting that a "massive body of pre-FISA case law" supports the conclusion that the legality of electronic surveillance should be determined on an *in camera, ex parte* basis); *Nicholson*, 955 F. Supp. at 592. In overturning a district court's order to disclose FISA materials to the defense, the *Daoud* Court described the belief that "adversary procedure is always essential to resolve contested issues of fact" as "an incomplete description of the American legal system in general and the federal judicial system in particular." 755 F.3d at 482.

There is only one reason to disclose the FISA materials to defense counsel. Title 50 U.S.C. § 1825(g) states that the Court must conduct its review of those materials *in camera* and *ex parte*, and disclosure is within the Court's discretion only following that review and only if

the Court is unable to determine the legality of the electronic surveillance, physical searches, or both, without the assistance of defense counsel. In *Duggan*, the court held that a district court is to conduct its review of the FISA materials *in camera* and *ex parte*, and only has discretion to disclose portions of those materials to the defense if it cannot make an accurate determination of the legality of the surveillance without disclosure to, and assistance from, defense counsel. 743 F.2d at 78. *Duggan*'s holding is fully supported by the legislative history of 50 U.S.C. § 1806(f) (and by extension 50 U.S.C. § 1825(g)), which states: "The court may order disclosure to [the defense] only if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance . . . . Once a judicial determination is made that the surveillance was lawful, a motion for discovery . . . must be denied." S. Rep. No. 95-701, 95th Cong., 2d Sess., 64-65 (1978) ("Senate Report").

By its terms, the defendant's motion to disclose the FISA materials is an effort to gather information that could be used to support his motion to suppress the FISA information. The defendant asserts that the "many potential grounds for suppression and extensive discovery materials with which the Court is unfamiliar" renders it "impossible" for the Court to "'make an accurate determination of the legality of the physical search,'" quoting 50 U.S.C. § 1825(g). (Def. Motion, p. 17). However, FISA's plain language precludes defense counsel from accessing the classified FISA materials to conduct a fishing expedition. In *Medunjanin*, the court noted that "[d]efense counsel . . . may not inspect the FISA dockets to construct a better argument for inspecting the FISA dockets. Such a circular exercise would be patently inconsistent with FISA. . . ." *Medunjanin*, 2012 WL 526428 at *10. The claim that the Court would need assistance from defense counsel is merely an attempt to circumvent the clear language of the statute, which unequivocally requires the Court to address the legality of the FISA surveillance first *in camera*

and *ex parte*. As the *Belfield* court stated: "Congress was adamant, in enacting FISA, that [its] 'carefully drawn procedure[s]' are not to be bypassed." *Belfield,* 692 F.2d at 146 (*citing* Senate Report at 63).

Courts are also in agreement that FISA's *in camera, ex parte* review does not violate the due process clause of the Fifth Amendment, nor does due process require that defendants be granted access to the FISA materials except as provided for in 50 U.S.C. § 1825(h). *See, e.g.*, *Megahey*, 553 F. Supp. at 1194; *Ott*, 827 F.2d at 476-477; *Gowadia*, 2009 WL 1649714 at *2; *ACLU Found.*, 952 F.2d at 465; *Nicholson*, 955 F. Supp. at 592 (The court found that based on "the unanimous holdings of prior case law, . . . FISA does not violate the Fifth or Sixth Amendments by authorizing *ex parte in camera* review."). The plain intention of 50 U.S.C. § 1825(h)—allowing the Court to order disclosure of material to which the defendants would be entitled under the Due Process Clause, such as material that had not been previously disclosed under *Brady v. Maryland*, 373 U.S. 83 (1963), even while ruling against the defendants' motion generally—cannot be interpreted to support the defendant's demand for access to all of the FISA materials in advance of the Court's *in camera, ex parte* review and determination of the legality of the collection.

2. A Security Clearance Does Not Entitle Defense Counsel to the FISA Materials

The defendant asserts that the fact that counsel has a security clearance means the Court should disclose the FISA materials subject to a protective order. (Def. Motion, p. 17). As discussed above, the sole statutory authority that grants a court discretion to disclose the FISA materials at this stage is set out at 50 U.S.C. § 1825(g), and this provision permits disclosure only where the court finds that it is unable to determine the legality of the physical search(es) based on its *in camera, ex parte* review alone and without the assistance of defense counsel.

Whether defense counsel holds an appropriate security clearance is irrelevant to the court's inquiry. *See Abu-Jihaad*, 630 F.3d at 129 (pursuant to FISA a district court must review *in camera* and *ex parte* the FISA materials and may only order disclosure to the extent required by due process).

In the FISA context, courts have consistently held that while holding a valid security clearance is a necessary prerequisite to reviewing classified information, it is not a sufficient basis for a court to order disclosure of classified information to defense counsel. Instead, cleared counsel have a "need to know" only if the Court determining the legality of the surveillance concluded that disclosure is "necessary." In *Bin Laden*, the court denied the disclosure of the FISA materials to cleared counsel, noting that "[d]efense counsel's [*sic*] assertion that, given their security clearances, they ought to have access to the sensitive documents is not persuasive to this Court. As the Government explains, those security clearances enable [co-defendant's] attorneys to review classified documents, 'but they do not entitle them to see all documents with that classification.'" 126 F. Supp. 2d at 287 n. 27, *aff'd by In re Terrorist Bombings in East Africa*, 552 F.3d 157 (2d Cir. 2008). The Ninth Circuit in *Ott* also rejected this argument, noting Congress's

> legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question, whether or not she happens for unrelated reasons to enjoy a security clearance. We reject the notion that a defendant's due process right to disclosure of FISA materials turns on the qualifications of his counsel.

827 F.2d at 476-77; *see also Nicholson*, 2010 WL 1641167, at *5 (referencing *Ott* and holding that "[b]ased on [the court's] *in-camera* review . . . the disclosure of FISA materials to [cleared] defense counsel is neither required nor appropriate"); *Al-Kidd v. Gonzalez,* 2008 WL 5123009

(D. Idaho 2008), at *7 ("despite plaintiff counsel's security clearances and therefore their ability to review sensitive information, the [*Ott*] court denied the plaintiff access to materials gathered pursuant to FISA. . . . [E]ven with a protective order and appropriate security clearances, this Court may still deny al-Kidd access to the information."); *Warsame*, 547 F.Supp.2d at 989 n.5; *El-Mezain*, 664 F.3d at 568.

Courts have repeatedly held that defense counsel are required to have more than a security clearance — defense counsel must also have a need to know. Most recently, the Seventh Circuit addressed the "need to know requirement" stating:

> [i]t's also a mistake to think that simple possession of a security clearance automatically entitles its possessor to access to classified information that he is cleared to see . . . . So in addition to having the requisite clearance the seeker must convince the holder of the information of the seeker's need to know it.

Daoud, 755 F.3d at 484.[23] "Getting clearance is not enough for access to classified information: there is quite sensibly, also a 'need to know' requirement. . . . Clearance simply qualifies counsel to view secret materials. It does not, however, *entitle* counsel to see anything and everything that the government has stamped classified even if it has something to do with a client." *United States v. Amawi*, 2009 WL 961143, at *1, 2 (N.D. Ohio 2009) (emphasis in original). *See also Medunjanin*, 2012 WL 526428, at *9 ("Defense counsel's security clearances add little to the case for disclosure. . . . As the government persuasively argues, unsealing the FISA materials in this case would provide the defense with unnecessary details of an extraordinarily sensitive anti-

[23] As the Seventh Circuit explained in *Daoud*, disclosing state secrets to cleared counsel could in fact harm national security because cleared counsel "might in their zeal to defend their client, to whom they owe a duty of candid communication, or misremembering what is classified and what is not, inadvertently say things that would provide clues to classified material." 755 F.3d at 484. The potential threat that classified information may be disclosed, even inadvertently, is further justification for the FISA materials to not be disclosed to cleared defense counsel.

terrorism investigation."); *United States v. Libby*, 429 F. Supp. 2d 18, 24 n. 8 (D.D.C. 2008) ("It is axiomatic that even if the defendant and his attorneys had been granted the highest level of security clearances, that fact alone would not entitle them to access to every piece of classified information this country possesses."). If this Court concludes from its *in camera, ex parte* review of the FISA materials that it is capable of accurately determining the legality of the FISA collection at issue, then no defense attorney, even one with an otherwise appropriate security clearance, would have a "need to know" any of the FISA materials.

The defendant's arguments in support of disclosure of the FISA materials have no basis in the law. In summary, the defendant is not entitled to the FISA materials for the purpose of challenging the lawfulness of the FISA authorities; the complete record presented to the FISC has been provided to this Court in a well-organized and straightforward manner, such that this Court is able to make a determination as to the legality of the FISA collection without the assistance of defense counsel; and defense counsel is not entitled to review the FISA materials simply because defense counsel possesses a security clearance. The Government respectfully submits that, therefore, there is nothing extraordinary about this case to justify an order to disclose the highly sensitive and classified FISA materials in this case under the applicable FISA standard. *See Rosen*, 477 F. Supp. 2d at 546 ("Review of the FISA applications, orders and other materials in this case presented none of the concerns that might warrant disclosure to the defense."). Accordingly, the defendant's motion for disclosure of the FISA materials should be denied.

VI. CONCLUSION: THERE IS NO BASIS TO DISCLOSE THE FISA MATERIALS OR TO SUPPRESS THE FISA INFORMATION

The defendant's motion should be denied. FISA's provisions for *in camera, ex parte* review comport with the due process requirements of the United States Constitution. *See, e.g.*,

Spanjol, 720 F. Supp. at 58-59; *United States v. Butenko*, 494 F.2d 593, 607 (3d Cir.), *cert. denied sub nom. Ivanov v. United States*, 419 U.S. 881 (1974); *Damrah*, 412 F.3d at 624; *Warsame*, 547 F. Supp. 2d at 988-89. The defendant advances no argument to justify any deviation from these well-established precedents.

The Attorney General has filed a declaration in this case stating that disclosure of the FISA materials or an adversary hearing would harm the national security of the United States. Therefore, FISA mandates that this Court conduct an *in camera, ex parte* review of the challenged FISA materials to determine whether the information was lawfully acquired and the physical search(es) was/were made in conformity with an order of authorization or approval. In conducting that review, the Court may disclose the FISA materials "only where such disclosure is necessary to make an accurate determination of the legality of the physical search." 50 U.S.C. § 1825(g). Congress, in enacting FISA's procedures for *in camera, ex parte* judicial review, has balanced and accommodated the competing interests of the Government and criminal defendants, and has articulated the proper standard for disclosure; that is, only where the Court determines that disclosure is necessary to the Court's accurate determination of the legality of the FISA collection.

The Court can make this determination without disclosing the classified and highly sensitive FISA materials to the defendant. The FISA materials at issue here are organized and readily understood, and an overview of them has been presented herein as a frame of reference. This Court will be able to render a determination based on its *in camera, ex parte* review, and the defendant has failed to present any colorable basis for supplanting Congress' reasoned judgment with a different proposed standard of review.

[CLASSIFIED MATERIAL REDACTED]

Even if this Court were to determine that the acquisition of the FISA information had not been lawfully acquired or that the physical search(es) was/were not made in conformity with an order of authorization or approval, the FISA evidence would nevertheless be admissible under the "good faith" exception to the exclusionary rule articulated in *Leon*, 468 U.S. 897. *See also Ning Wen*, 477 F.3d at 897 (holding that the *Leon* good-faith exception applies to FISA orders); *Mubayyid*, 521 F. Supp. 2d at 140 n. 12 (noting that the Government could proceed in good-faith reliance on FISA orders even if FISA were deemed unconstitutional); *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n. 8; *Nicholson*, 2010 WL 1641167, at *6.

Based on the foregoing analysis, the Government respectfully submits that the Court must conduct an *in camera*, *ex parte* review of the FISA materials and the Government's classified submission and should: (1) find that the physical search(es) at issue in this case was/were both lawfully authorized and lawfully conducted; (2) hold that disclosure to the defendant of the FISA materials and the Government's classified submission is not authorized because the Court is able to make an accurate determination of the legality of the physical search(es) without disclosing the FISA materials or any portions thereof; (3) hold that the fruits of physical search(es) should not be suppressed; (4) order that the FISA materials and the

Government's classified submissions be maintained under seal by the Court Security Officer or his or her designee; and find that no hearing is necessary.[24]

DATED: September 23, 2016

Respectfully submitted,

PREET BHARARA
United States Attorney

//S//
BRENDAN QUIGLEY
Assistant United States Attorney

NEGAR TEKEEI
Assistant United States Attorney

ANDREW DEFILIPPIS
Assistant United States Attorney

[24] A district court order granting motions or requests under 50 U.S.C. § 1825(h), a decision that the physical search(es) was/were not lawfully authorized or conducted, and an order requiring the disclosure of FISA materials is each a final order for purposes of appeal. 50 U.S.C. § 1825(i). Should the Court conclude that disclosure of any item within any of the FISA materials or suppression of any FISA-obtained or -derived information may be required, given the significant national security consequences that would result from such disclosure or suppression, the Government would expect to pursue an appeal. Accordingly, the Government respectfully requests that the Court indicate its intent to do so before issuing any order, and that the Court stay any such order pending an appeal by the United States of that order.